DATA CENTER INTRUSION PREVENTION SYSTEM COMPARATIVE REPORT

Security Value Map™ (SVM)

Authors – Thomas Skybakmoen, Keith Bormann, Morgan Dhanraj

Tested Products

Fortinet FortiGate 3000D v5.4.0, build 7184

HPE TippingPoint S7500NX v3.7.2.4252

IBM Security Network Protection XGS 7100 v5.3.2.1

Intel Security McAfee Network Security Platform NS9100 v8.2.5.120

Juniper Networks SRX5400 v12.3X48-D18

Palo Alto Networks PA-7050 v7.0.4

Environment

Data Center Intrusion Prevention System: Test Methodology v2.0

Overview

Empirical data from individual Test Reports and Comparative Reports is used to create NSS Labs' unique Security Value Map™ (SVM). The SVM illustrates the relative value of security investment options by mapping the *Security Effectiveness* and the *Total Cost of Ownership (TCO) per Protected Mbps* (*Value*) of tested product configurations. The terms *TCO per Protected Mbps* and *Value* are used interchangeably throughout the Comparative Reports.

The SVM provides an aggregated view of the detailed findings from NSS' group tests. Individual Test Reports are available for each product tested. Comparative Reports provide detailed comparisons across all tested products in the following areas:

- Security
- Performance
- TCO

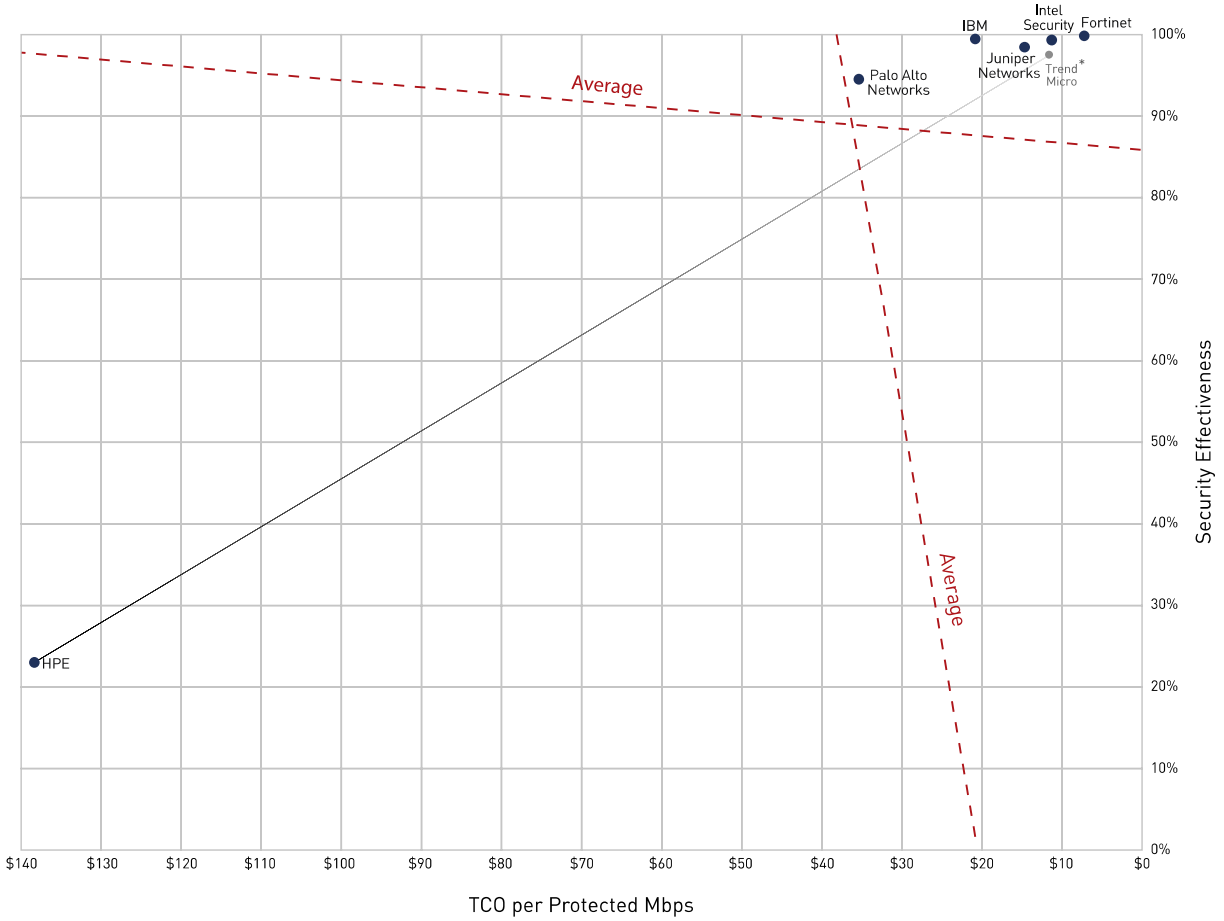

Figure 1 – NSS Labs' 2016 Security Value Map (SVM) for Data Center Intrusion Prevention System (DCIPS)

* On March 1, 2016, TippingPoint, owned by Hewlett Packard Enterprise (HPE), submitted the S7500NX v3.7.2.4252 to the NSS Labs DCIPS Public Group Test. During testing, NSS discovered a number of security issues, which caused the product to receive a Caution rating. After testing began, Trend Micro finalized the acquisition of TippingPoint from HPE (March 8, 2016). As the new owner of TippingPoint, Trend Micro was made aware of the test results. Trend Micro quickly took action, resolved the issues, and provided NSS with a late submission for

testing. NSS confirmed TOS v3.8.3.4494 resolved the security issues found in the HPE version of the product, and also improved both *Security Effectiveness* and performance (see individual Test Report). The NSS Security Value Map™ (SVM) is a point-in-time measurement, and due to the timing of the acquisition, the HPE version of the product is represented in the SVM. However, in light of these unusual circumstances, we have included this notation to inform our enterprise clients of the corrective actions taken by Trend Micro.

Key Findings

- Overall *Security Effectiveness* ranged between 23.2% and 99.9%, with four of the six tested products achieving a rating greater than 98.6%.
- *TCO per Protected Mbps* ranged between US$7 and US$138, with most tested solutions costing less than US$22 per protected Mbps.
- The average *Security Effectiveness* rating was 85.8%; five devices received an above-average *Security Effectiveness* rating, and one received a below-average *Security Effectiveness* rating.
- The average *TCO per Protected Mbps* was US$ $38; five devices were rated as having above-average value; one was rated as having below-average value.

Product Rating

The Overall Rating in Figure 2 is determined by which section of the SVM the product falls within: *Recommended* (top right), *Neutral* (top left or bottom right), or *Caution* (bottom left). For more information on how the SVM is constructed, see the *How to Read the SVM* section of this document.

Product	Security Effectiveness		Value in US$ (TCO per Protected Mbps)		Overall Rating
Fortinet FortiGate 3000D	99.9%	Above average	$7	Below average	Recommended
HPE TippingPoint S7500NX	23.2%	Below average	$138	Above average	Caution
IBM XGS 7100	99.6%	Above average	$21	Below average	Recommended
Intel Security McAfee NS9100	99.4%	Above average	$12	Below average	Recommended
Juniper Networks SRX5400	98.7%	Above average	$15	Below average	Recommended
Palo Alto Networks PA-7050	94.2%	Above average	$35	Below average	Recommended

Figure 2 – NSS Labs' 2016 Recommendations for Data Center Intrusion Prevention System (DCIPS)

This report is part of a series of Comparative Reports on security, performance, TCO, and the SVM. In addition, NSS clients have access to an NSS Labs *SVM Toolkit™* that allows for the incorporation of organization-specific costs and requirements to create a completely customized SVM. For more information, visit www.nsslabs.com.

Table of Contents:

Table of Figures

How to Read the SVM

The SVM depicts the value of a typical deployment of four DCIPS products plus one central management unit (and where necessary, a log aggregation and/or event management unit). Running a multi-device deployment provides a more accurate reflection of cost than running only a single DCIPS.

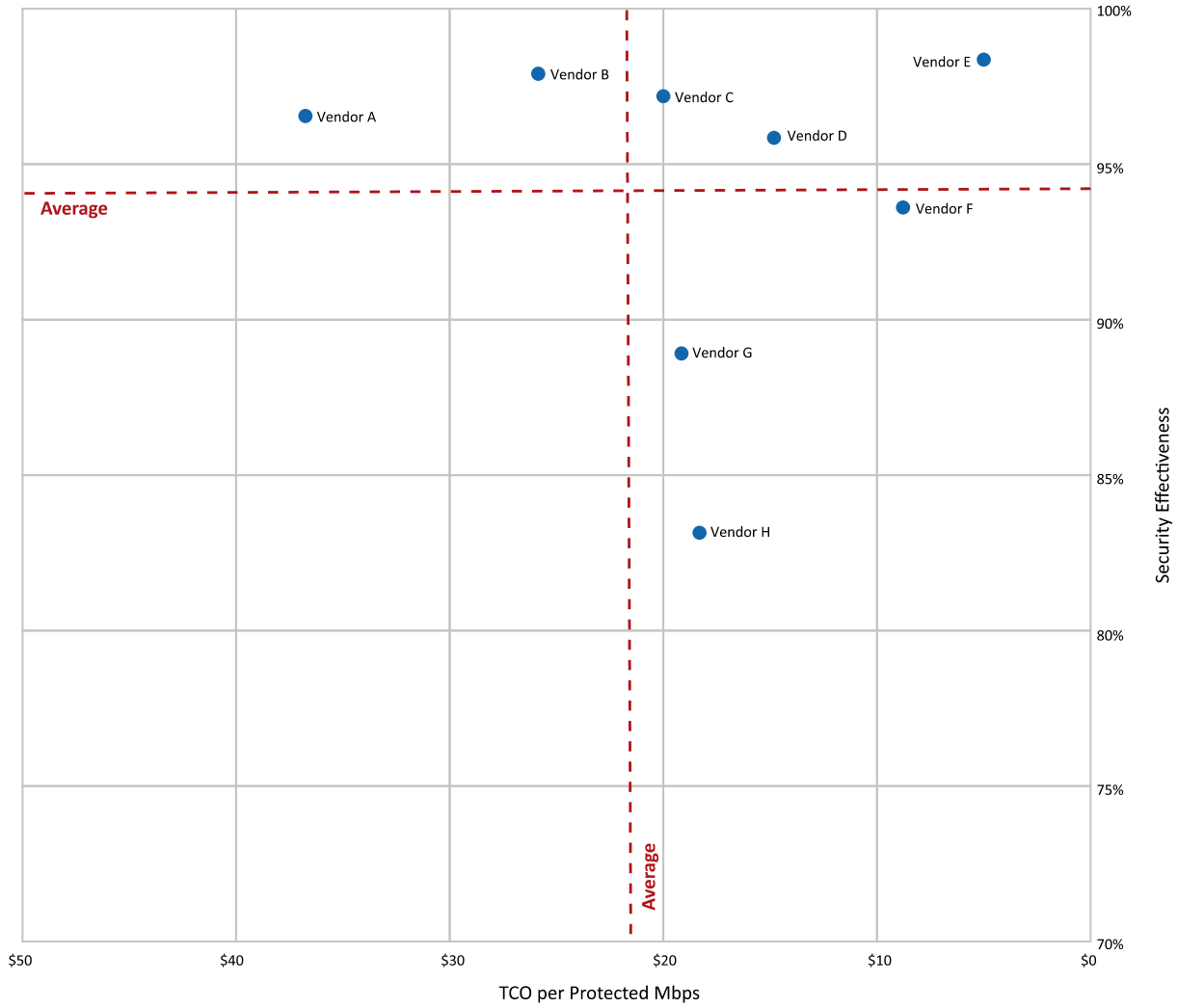

Figure 3 – Example SVM

No two security products deliver the same security effectiveness or performance, making precise comparisons extremely difficult. In order to enable value-based comparisons of DCIPS products on the market, NSS has developed a unique metric: *TCO per Protected Mbps.*

The *x* axis displays the *TCO per Protected Mbps* in US dollars, which decreases from left to right. This metric incorporates the 3-Year TCO with the *Security Effectiveness* score to provide a data point with which to compare the actual value of each product tested. The formula used is as follows: 3-Year TCO/ (*Security Effectiveness* x *NSS-Tested Throughput*). The TCO incorporates capital expenditure (capex) costs over a three-year period, including initial acquisition and deployment costs and annual maintenance and update costs (software and hardware updates). For more details on *Security Effectiveness* and TCO, see the Security and TCO comparative reports at www.nsslabs.com.

The *y* axis displays the *Security Effectiveness* score as a percentage. *Security Effectiveness* is greater toward the top of the *y* axis. Devices that are missing critical security capabilities will have a reduced *Security Effectiveness* score.

The SVM displays two dotted lines that represent the average *Security Effectiveness* and *TCO per Protected Mbps* of all the tested products. These lines divide the SVM into four unequally sized sections. Where a product's *Security Effectiveness* and *TCO per Protected Mbps* scores map on the SVM will determine which section it falls into:

- **Recommended**: Products that map into the upper-right section of the SVM score well for both *Security Effectiveness* and *TCO per Protected Mbps***.** These products provide a high level of detection and value for money.
- **Caution:** Products that map into the lower-left section of the SVM offer limited value for money given their 3-Year TCO and measured *Security Effectiveness*.
- **Neutral:** Products that map into either the upper-left or lower-right sections may be good choices for organizations with specific security or budget requirements.

Neutral products in the upper-left section score as above average for *Security Effectiveness* but below average for *TCO per Protected Mbps (Value)*. These products are suitable for environments requiring a high level of detection, albeit at a higher-than-average cost.

Conversely, *Neutral* products in the lower-right section score as below average for *Security Effectiveness* but above average for *TCO per Protected Mbps (Value).* These products would be suitable for environments where a slightly lower level of detection is acceptable in exchange for a lower TCO.

In all cases, the SVM should only be a starting point. NSS clients have access to the *SVM Toolkit*, which allows for the incorporation of organization-specific costs and requirements to create a custom SVM. Clients can also meet with NSS analysts if they wish to develop a custom SVM.

Analysis

Each product may fall into one of three categories based on its rating in the SVM: *Recommended*, *Neutral*, or *Caution*. Each of the tested products receives only a single rating. Vendors are listed alphabetically within each section.

Recommended

Fortinet FortiGate 3000D v5.4.0, build 7184

Block Rate	The Fortinet FortiGate 3000D blocked 99.9% of exploits.
Evasion Techniques	The device proved effective against all evasion techniques tested.
Stability and Reliability	The device passed all stability and reliability tests.
Performance Rating	The Fortinet FortiGate 3000D is rated by NSS at 11.042 Gbps, which is lower than vendor-claimed performance; Fortinet rates this device at 20 Gbps.

IBM Security Network Protection XGS 7100 v5.3.2.1

Block Rate	The IBM XGS 7100 blocked 99.6% of exploits.
Evasion Techniques	The device proved effective against all evasion techniques tested.
Stability and Reliability	The device passed all stability and reliability tests.
Performance Rating	The IBM XGS 7100 is rated by NSS at 25.949 Gbps, which is above vendor-claimed performance; IBM rates this device at 25 Gbps.

Intel Security McAfee Network Security Platform NS9100 v8.2.5.120

Block Rate	The McAfee NS9100 blocked 99.4% of exploits.
Evasion Techniques	The device proved effective against all evasion techniques tested.
Stability and Reliability	The device passed all stability and reliability tests.
Performance Rating	The McAfee NS9100 is rated by NSS at 19.949 Gbps, which is higher than vendor-claimed performance; Intel Security rates this device at 10 Gbps.

Juniper Networks SRX5400 v12.3X48-D18

Block Rate	The Juniper Networks SRX5400 blocked 98.7% of exploits.
Evasion Techniques	The device proved effective against all evasion techniques tested.
Stability and Reliability	The device passed all stability and reliability tests.
Performance Rating	The Juniper Networks SRX5400 is rated by NSS at 10.884 Gbps, which is lower than the vendor-claimed performance; Juniper Networks rates this device at 22 Gbps.

Palo Alto Networks PA-7050 v7.0.4

Block Rate	The Palo Alto Networks PA-7050 blocked 94.2% of exploits.
Evasion Techniques	The device proved effective against all evasion techniques tested.
Stability and Reliability	The device passed all stability and reliability tests.
Performance Rating	The Palo Alto Networks PA-7050 is rated by NSS at 30.375 Gbps, which is lower than vendor-claimed performance; Palo Alto Networks rates this device at 60 Gbps.

Neutral

NA

No Product received a *Neutral* rating in this round of testing.

Caution

HPE TippingPoint S7500NX v3.7.2.4252

Block Rate	The HPE TippingPoint S7500NX blocked 97.9% of exploits.
Evasion Techniques	The device failed to protect against the following evasion technique: IP Fragmentation + MSRPC Fragmentation
Stability and Reliability	The device also failed the following stability and reliability tests: Behavior of the state engine under load (Normal and Maximum Exceeded Loads).
Performance Rating	The HPE TippingPoint S7500NX is rated by NSS at 12.525 Gbps, which is lower than vendor-claimed performance; HPE TippingPoint rates this device at 20 Gbps.

Test Methodology

Data Center Intrusion Prevention System v2.0

A copy of the test methodology is available on the NSS Labs website at www.nsslabs.com.

Contact Information

NSS Labs, Inc.
206 Wild Basin Road
Building A, Suite 200
Austin, TX 78746
info@nsslabs.com
www.nsslabs.com